



~~Docket No. 43521-0700~~

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of:

Examiner: TBA

Hidema TANAKA et al.

Group Art Unit: TBA

Serial No.: 10/622,722

January 26, 2004

Filed: July 18, 2003

Irvine, California 92614

## **INFORMATION DISCLOSURE STATEMENT**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

In an attempt to fully comply with the duty of disclosure set forth in 37 C.F.R. § 1.56 and in conformance with 37 C.F.R. §§ 1.97 and 1.98, applicant wishes to bring to the attention of the U.S. Patent Office the following references:

Babbage & Frisch "On MISTY1 Higher Order Differential Cryptanalysis"  
Daemen, Knudsen & Rijmen "The Block Cipher SQUARE"  
Jakobsen & Knudsen "The Interpolation Attack on Block Cipher"  
Nyberg & Knudsen, "Provable Security Against Differential Cryptanalysis"  
Shimoyama, Moriai & Kaneko, "Improving the Higher Order Differential Attack and Cryptanalysis of the KN Cipher"  
Tanaka, Hisamatsu & Kaneko, "Strength of MISTY1 without FL Function for Higher Order Differential Attack"

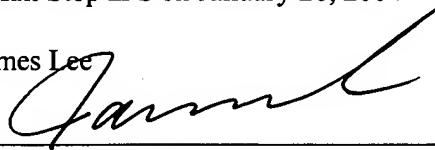
Copies of these references and a form PTO-A820 are attached.

Docket No. 43521-0700

If the Examiner believes that a telephone conference would help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, Mail Stop IDS on January 26, 2004

by: James Lee



Signature

Date of Signature: January 26, 2004

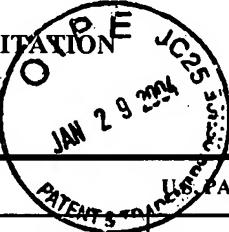
Very truly yours,

SNELL & WILMER LLP



Joseph W. Price, Reg. No. 25,124  
1920 Main Street, Suite 1200  
Irvine, CA 92614  
949/253-4924

<b>INFORMATION DISCLOSURE CITATION</b> <small>(Use several sheets if necessary)</small>			Docket Number (Optional) <b>43521-0700</b>		Application Number <b>10/622,722</b>		
			Applicant(s) <b>Hideya TANAKA, T shinobu KANEKO</b>		Filing Date <b>July 18, 2003</b>		Group Art Unit <b>TBA</b>
 <b>U.S. PATENT DOCUMENTS</b>							
*EXAMINER INITIAL	REF	DOCUMENT NUMBER	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE	
<b>FOREIGN PATENT DOCUMENTS</b>							
REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	<b>Translation</b>	
						YES	NO
<b>OTHER DOCUMENTS</b> <i>(Including Author, Title, Date, Pertinent Pages, Etc.)</i>							
		Babbage & Frisch, "On MISTY1 Higher Order Differential Cryptanalysis," 3rd International Conference on Information Security and Cryptology ICISC 2000, Seoul, Korea, December 8-9, 2000 (pp 22-36)					
		Daemen, Knudsen & Rijmen "The Block Cipher SQUARE", 4th International Workshop FSE '97 on Fast Software Encryption, Haifa, Israel, January 20-22, 1997 (Eli Biham ed.) (pp 149-165)					
<b>EXAMINER</b>			<b>DATE CONSIDERED</b>				

<b>INFORMATION DISCLOSURE CITATION</b> <i>(Use several sheets if necessary)</i>			Docket Number (Optional) <b>43521-0700</b>		Application Number <b>10/622,722</b>		
			Applicant(s) <b>Hidema TANAKA, Toshinobu KANEKO</b>				
Filing Date <b>July 18, 2003</b>			Group Art Unit <b>TBA</b>				
<b>U.S. PATENT DOCUMENTS</b>							
*EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
<b>FOREIGN PATENT DOCUMENTS</b>							
REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Translation	
						YES	NO
<b>OTHER DOCUMENTS</b> <i>(Including Author, Title, Date, Pertinent Pages, Etc.)</i>							
		Jakobsen & Knudsen "The Interpolation Attack on Block Cipher," FSE-4th International Workshop LNCS 1008					
		Nyberg, Knudsen, "Provable Security Against Differential Cryptanalysis," Journal of Cryptology, Vol. 8-no. 1					
<b>EXAMINER</b>				<b>DATE CONSIDERED</b>			
<b>EXAMINER:</b> Initial if citation considered, whether or not citation is in conformance with MPEP Section 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.							

